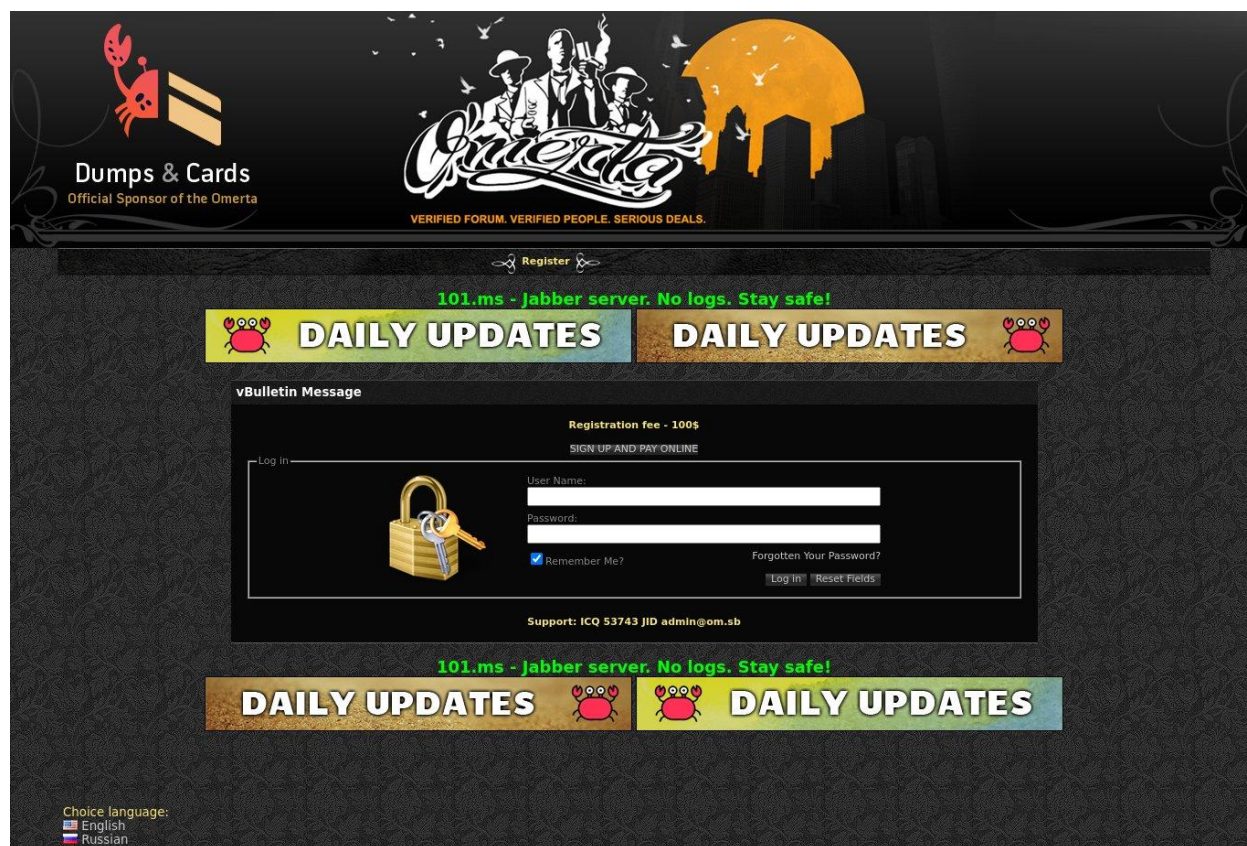


00. Exposing a Boutique Fraudulent and Rogue Cybercrime-Friendly Forum Community - An Analysis

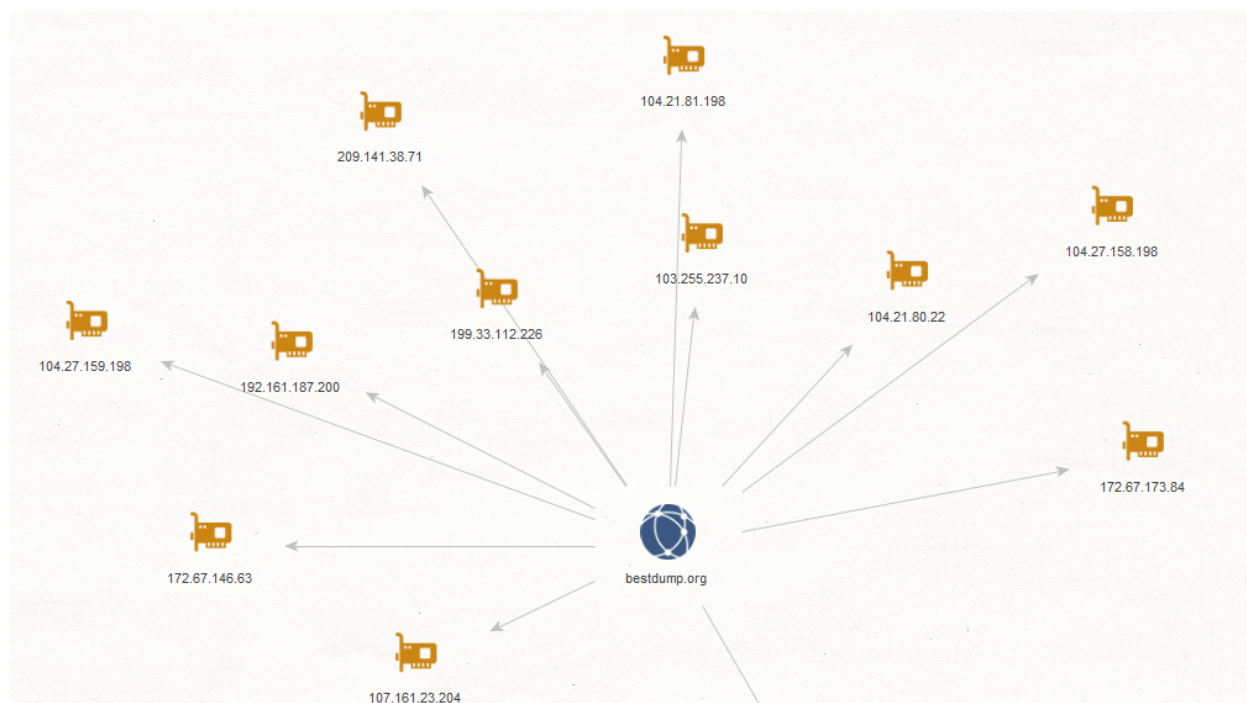


Sample screenshot of the `hxxp://omerta.cc` cybercrime-friendly forum parked on the same IP as the original E-Shop for stolen credit cards information

We've decided to take an in-depth look inside the infamous `hxxp://omerta.cc` cybercrime-friendly forum community which is currently sharing the same infrastructure as the original E-Shop for stolen credit cards information which we've already profiled and elaborated more in two separate white papers and case studies where I've decided to continue monitoring and investigating the original E-Shop for stolen credit cards information which we profiled in our original white paper - `hxxp://thefreshstuffs.at` and came up with some pretty interesting results which also include an additional set of E-shops for stolen credit card information that are actively sharing the same infrastructure of the original E-Shop for stolen credit card information which we profiled in our original research.

In this analysis we'll provide actionable intelligence on the bulletproof hosting infrastructure behind the recently discovered E-Shops for stolen credit card information including actionable intelligence and personally identifiable information on the actual cybercrime-friendly forum owners with the idea to assist researchers and vendors on their way to track down and monitor this campaign for related malicious and fraudulent activity.

During our initial analysis of the infamous cybercrime-friendly forum we've found an additional set of clues which appear to be a bulletproof hosting infrastructure that's also currently hosting a variety of related E-Shops for stolen and compromised credit card information which we'll profile in this analysis and offer an in-depth peek inside the actual infrastructure that's supporting these E-Shops for stolen credit card information.



Sample name servers involved in this campaign that are currently responding for managing and running the related domains which we found using Maltego and WhoisXML API's integration:

- hxxp://omertadns.biz
 - hxxp://omerta.ws
 - hxxp://NS1.CRYSTALDUMPS.RU
 - hxxp://NS2.CRYSTALDUMPS.RU

It also appears that the actual E-Shop for stolen credit cards information which we profiled in our original analysis is also sharing the same infrastructure with the cybercrime-friendly forum community which we'll profile in this post including related malicious activity where we'll offer practical and actionable intelligence in terms of offering researchers and vendors the opportunity to track down and monitor the campaign including the actual bulletproof hosting provider.

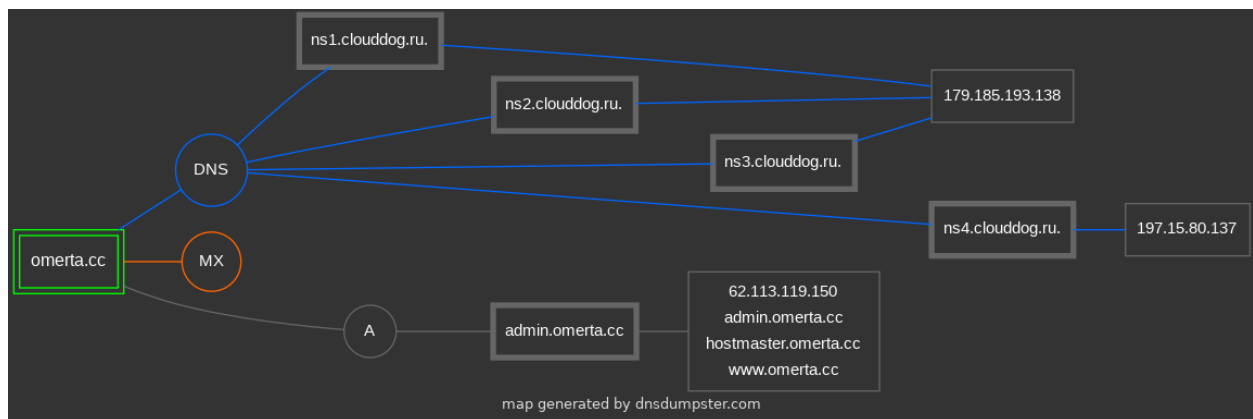
Sample domains involved that are currently sharing the same bulletproof hosting infrastructure part of this campaign:

hxxp://thefreshstuffs.at -> hxxp://omerta.cc

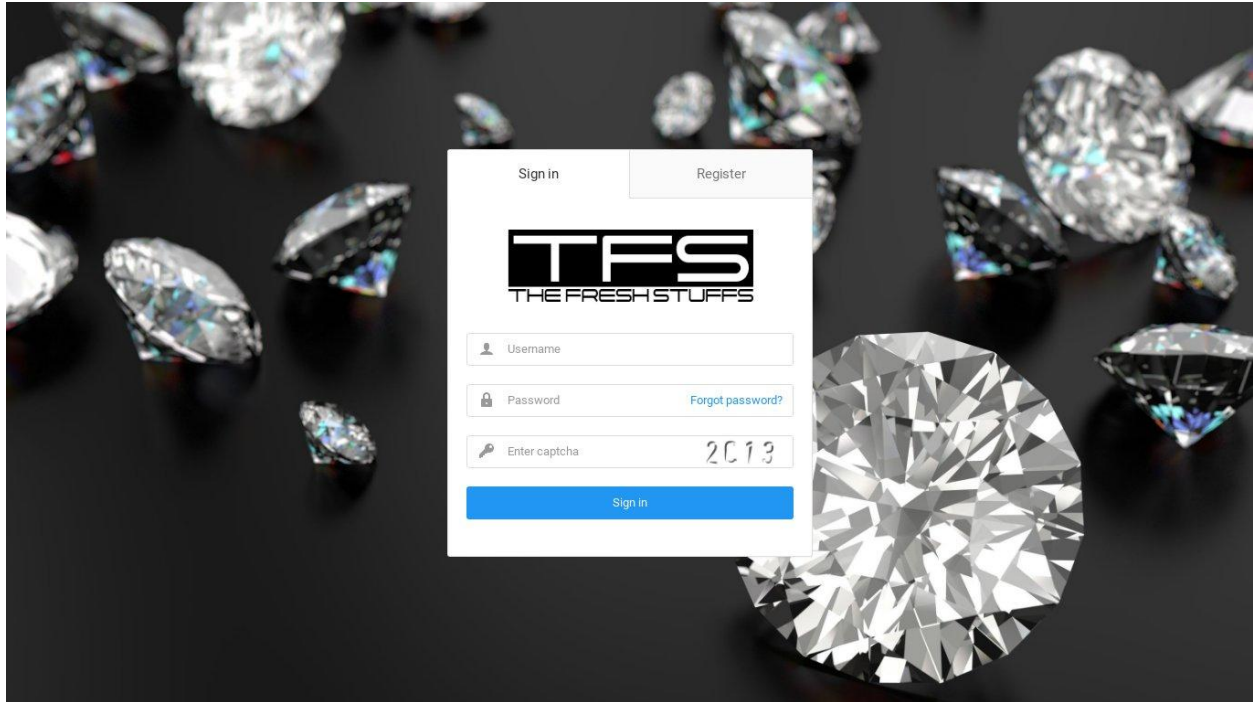
- 91-139-196-113.plvd.ddns.bulsat.com - 91.139.196.113

Sampe malicious and fraudulent domains known to be currently responding to the same IPs as hxxp://omerta.ws:

hxxp://0-giochi.ws
hxxp://0000opengate2.ws
hxxp://00063.entelit.ws
hxxp://001.12345678.ws
hxxp://001.mcard.ws
hxxp://001af2e3-990d-420f-b3cc-d7cf89f1ca8e.client.pbx.ws
hxxp://002.mcard.ws
hxxp://003.mcard.ws
hxxp://0030.ws
hxxp://004.mcard.ws



Sample Passive DNS response for the infamous hxxp://omerta.cc cybercrime-friendly forum community



Sample Screenshot of a Rogue and Malicious Online E-Shop for Selling Stolen Credit Cards Information

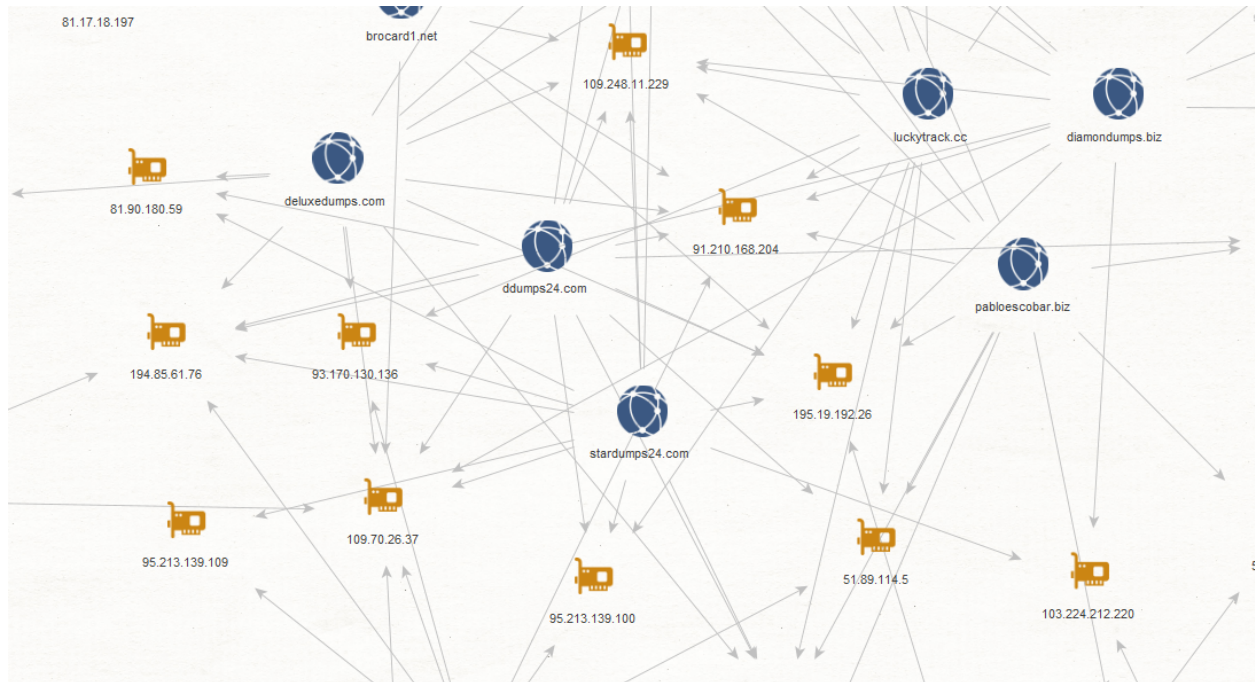
Name Servers:

hxxp://A.perfekttrain.org
hxxp://B.perfekttrain.org
hxxp://C.perfekttrain.org
hxxp://D.perfekttrain.org

Related online E-shops for stolen credit cards hosted on the same infrastructure:

briansclub.at
briansclub.cm
brians.shop
brocard1.net
buybestbiz.net
swipebz.org
swipebz.net
goodshopbiz.net
buybestbiz.net
buybest.cc
buybest.pro
c2bit.pw
gocvv.su
c2bit.su
c2bit.pw

c2bit.pw
gocvv.su
c2bit.su
c2bit.pro
c2bit-power.pw
vrf-apple.com
carderbay.com
cardhouse.cc
ddumps24.com
deluxedumps.com
diamondumps.biz
ebin.cc
entershop.st
fe-shop.link
flyded.gs
freshstuff24.net
fullzshop.su
fullzstore.su
goldenshop.cc
goodshopbiz.net
greendumps24.biz
kingven.cc
luckytrack.cc
mrwhite.biz
pabloescobar.biz
russianmarket.gs
russianmarket.zone
shadowcarders.com
smd1.la
stardumps24.com
tiesto.ec
topcc.store
vendta.cc
worldcvv.me
wt1.la
wt1shop.org
www.fe-acc18.ru
yohohobay.cc
swipe.bz



Sample related malicious domains known to have interacted and are currently interacting with the same hosting infrastructure:

kingven.cc
 goldenshop.cc
 beranielmenc.com
 mrwhite.biz
 bumpogrides.men
 greendumps24.biz
 russianmarket.gs
 banessionia.men
 luckytrack.cc
 shadowcarders.com
 pabloescobar.biz
 stardumps24.com
 russianmarket.zone
 topcc.store
 smd1.la
 briansclub.at
 tiesto.ec
 brocard1.net
 bestdumps.biz
 www.longbucks.com
 www.forexpeacearmy.com

fullzstore.su
goodshopbiz.net
fullzshop.su
wt1.la
liberiaconfidential.wordpress.com
wt1shop.org
yohohobay.cc
swipe.bz
c2bit.pw
briansclub.cm
cardhouse.cc
buybestbiz.net
deluxedumps.com
carderbay.com
ebin.cc
ddumps24.com
fe-shop.link
diamondumps.biz
freshstuff24.net
the-airmoney.ru
entershop.st
bestdump.org
flyded.gs
vendta.cc
worldcvv.me
grayget.webcam
orangeizer.men
coachlointe.men
browntor.trade
grayator.webcam
brownment.trade
consolefoundry.date
golden03.org
pinkget.win
consoleform.date
orangetor.men
doerkennaw.bid
pinkator.win

IM Observatory server report for 100500.cc

Test started 2019-03-31 08:57:41 UTC 2 years ago.

[Show client to server result](#) | [Permalink to this report](#) |

Retest

Score

100500.cc:5269



Grade:

A

Sample related malicious and fraudulent IPs known to be part of the bulletproof hosting provider's infrastructure that are currently responsible for offering hosting services to the E-Shops for stolen credit cards information which we profiled in this analysis:

35.199.65.220
129.226.192.109
35.188.45.236
78.41.204.33
78.41.204.29
78.41.204.38
78.41.204.35
78.41.204.34
78.41.204.28
78.41.204.31
78.41.204.30
35.234.120.206
35.242.170.33
35.205.152.183
35.246.16.37
35.246.78.112
35.241.199.75
35.228.99.65
8.209.73.178
35.198.175.43

195.19.192.26
104.27.152.51
109.248.11.229
190.115.18.200
172.67.211.232
104.27.153.51
46.173.219.103
104.27.165.81
156.234.71.98
104.27.164.81
104.21.85.119
172.67.205.151
78.41.204.37
5.79.68.103
78.41.204.26
209.126.123.12
81.90.180.59
185.22.152.157
104.24.105.8
31.220.2.84
8.208.77.140
104.24.104.8
198.144.121.105
169.47.130.88
104.27.157.214
169.47.130.87
104.27.156.214
104.18.47.175
169.47.130.86
104.27.144.53
169.47.130.85
104.27.145.53
104.18.46.175
169.47.130.83
104.27.134.138
172.67.180.56
169.47.130.84
172.67.211.134
104.21.51.63
169.47.130.81
172.64.165.26
172.67.222.226
169.47.130.82
104.27.135.138

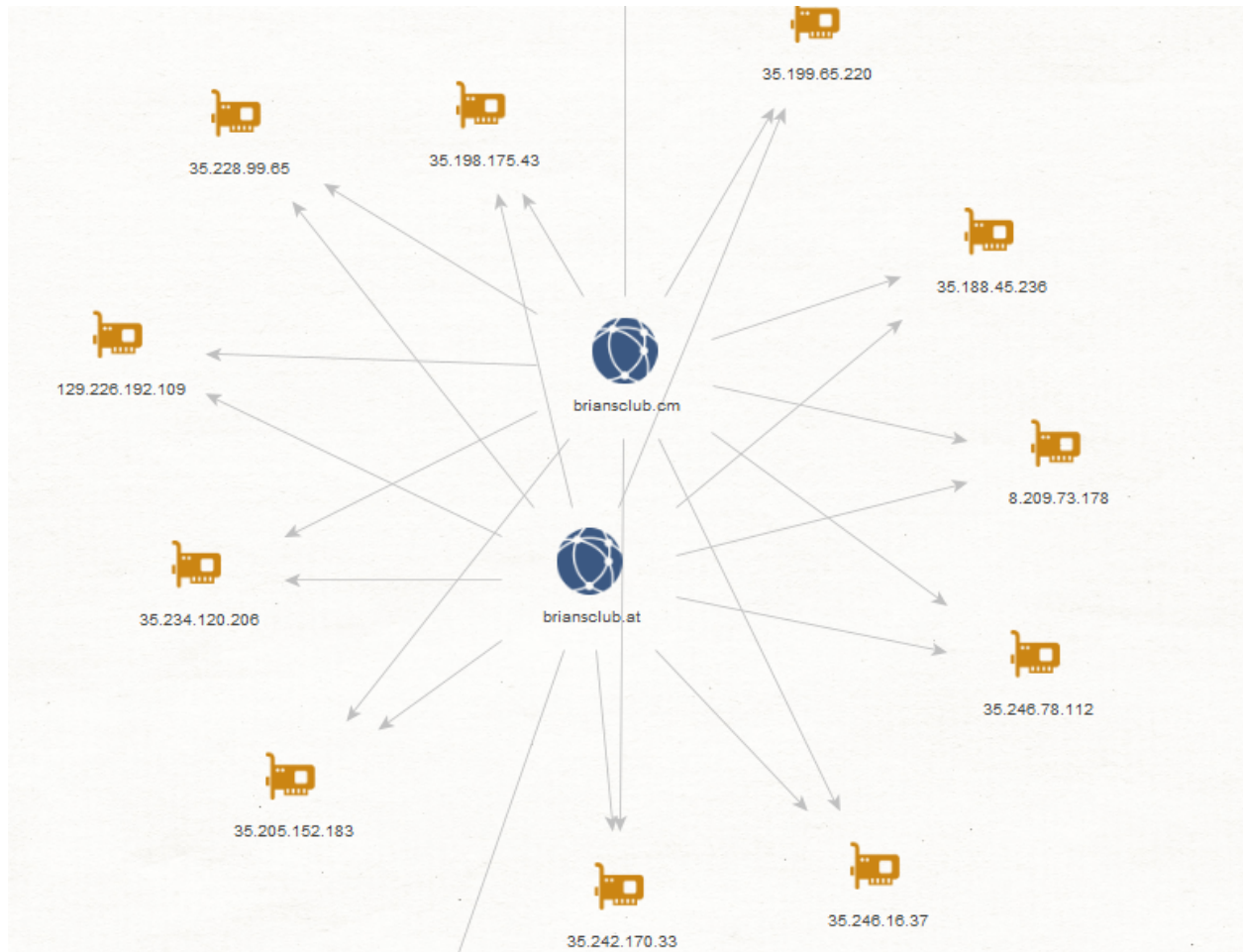
169.47.130.79
104.21.60.33
169.47.130.80
172.64.164.26
172.67.191.31
185.207.204.211
185.145.128.177
104.18.37.167
77.72.0.126
185.254.188.237
104.18.36.167
45.33.20.235
124.156.183.249
72.14.185.43
119.28.57.199
104.243.45.179
45.33.30.197
124.156.188.168
103.224.212.222
93.187.129.248
72.14.178.174
119.28.30.152
119.28.49.50
185.143.223.153
103.239.29.151
194.67.71.148
173.255.194.134
185.178.208.185
104.23.128.56
185.173.179.173
104.23.129.56
103.9.77.212
109.248.11.61
89.111.167.3
95.213.139.100
49.51.132.214
93.170.130.136
104.27.167.155
210.56.60.227
51.89.114.5
104.27.166.155
185.38.142.78
45.33.18.44
194.67.71.21

104.27.140.117
172.67.146.17
104.27.141.117
104.21.63.139
91.92.70.18
95.213.139.109
95.181.178.236
36.110.114.130
185.132.53.221
91.210.168.204
198.105.254.11
185.132.53.231
109.70.26.37
82.151.108.118
194.85.61.76
185.132.53.219
111.90.149.200
72.52.178.23
104.18.43.18
111.90.138.208
50.19.83.33
172.67.220.21
172.67.186.21
199.59.242.153
104.18.42.18
91.195.240.117
111.90.159.60
111.90.158.115
185.35.137.50
192.187.111.219
192.187.111.222
81.17.18.197
185.11.145.111
192.187.111.220
185.61.137.47
192.187.111.221
185.107.56.200
185.107.56.199
206.221.176.184
104.27.183.84
185.107.56.198
104.27.182.84
45.33.2.79
104.28.30.74

37.48.65.149
104.28.31.74
198.58.118.167
172.67.132.84
96.126.123.244
172.67.132.168
45.56.79.23
104.28.22.69
45.33.23.183
104.28.23.69
70.32.1.32
104.18.39.6
45.79.19.196
172.67.222.148
104.21.38.117
104.18.38.6
5.23.54.176
172.67.146.63
77.244.219.37
103.255.237.10
104.21.81.198
52.0.217.44
111.90.141.122
185.11.145.5
103.155.93.116
103.155.93.184
104.27.158.198
104.27.159.198
192.161.187.200
172.67.173.84
209.141.38.71
107.161.23.204
188.225.9.25
104.21.80.22
199.33.112.226
81.90.180.214
103.224.212.220
170.178.168.203
35.203.17.246
185.107.56.52
162.210.195.123
192.157.56.142
207.244.67.139
207.244.67.138

162.210.196.166
162.210.195.122
162.210.199.65
192.157.56.141
162.210.199.87
185.99.133.188
46.249.59.121
104.24.101.187
47.254.216.171
104.24.100.187
104.28.27.206
172.67.152.209
190.115.18.179
45.9.148.209
1.1.1.1
190.115.18.186
31.202.2.61
31.220.2.61
91.241.19.61
185.104.114.189
94.242.224.214
185.99.133.68
185.162.11.77
185.77.128.109
185.20.185.228
188.209.49.192
104.247.81.13
188.209.49.71
185.161.209.58
45.9.150.24
149.3.170.39
104.18.54.149
104.18.55.149
185.61.137.58
185.255.179.78
81.177.23.102
185.61.137.52
185.219.42.117
185.135.83.120
78.24.223.204
185.244.43.42
185.115.140.154
185.20.187.160
3.13.31.214

5.8.76.180
88.212.253.133
208.69.117.124
151.248.123.92
185.180.198.111
5.188.9.54
194.67.104.103
185.11.145.249
104.27.128.248
185.62.190.13
185.61.137.99
104.27.129.248
172.67.159.6
190.115.21.170
104.21.58.107
185.61.137.49
91.220.101.41
107.150.98.48
104.28.22.40
179.43.176.223
172.67.130.129
104.28.23.40
104.21.3.85
47.74.0.181
47.74.8.123
64.32.8.69
46.166.182.113
64.32.8.68
185.107.56.59
63.143.32.85
64.32.8.67
185.107.56.58
185.107.56.57
63.143.32.89
64.32.8.70
185.107.56.60
63.143.32.91



We'll continue monitoring the bulletproof hosting provider's infrastructure and will post updated including to offer actionable intelligence behind its infrastructure including some of its clients and customers which include a variety of cybercrime-friendly forums and various E-Shops for stolen and compromised credit cards information.